Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 9 | Issue : 3 | Mar 2023

# SECURE ENCRYPTED MOBILE : USER REQUIREMENT AND POLICY CONSTRAINTS

Ayan Dhanda

Undergraduate Student, Computer Science Engineering, International Centre for Applied Sciences (ICAS), Manipal Academy of Higher Education (MAHE).

## ABSTRACT

There is no stop to technology, every day new tools or techniques are emerging, and with the increase in technologies and use of mobile devices, digital crimes are also increasing. Companies are starting to face an enormous amount of data loss. The world is run by technology and networks and it becomes important for everyone to understand that cyber security, company assets, or the individual's data are at risk without the protection added to it. The usage of business applications on mobile devices has become common to keep the production environment active. IT companies use updated technologies to protect their data, but attackers are always enhancing new techniques to break through these technologies. Cyber Security becomes important to make sure the assets, information/data, and personal or financial details are safeguarded and not at risk. This paper aims to review the threats and crimes involving mobile devices and discuss the requirement of secure mobile phones including policy constraints of various governments owing to posing significant challenges to public safety.

### 1. Introduction

The future of computers and communication lies with mobile devices, such as laptops, tablets and smartphones with desktop-computer capabilities. Their size, operating systems, applications and processing power make them ideal to use from any place with an internet connection. And with the expansion of ruggedized devices, the Internet of Things (IoT) and operating systems, such as Chrome OS, mac OS and Windows 10, every piece of hardware that's enhanced with this software and capabilities becomes a mobile computing device. Because mobile devices have become more affordable and portable, organizations and users have preferred to buy and use them over desktop computers. And with ubiquitous wireless internet access, all varieties of mobile devices are becoming more vulnerable to attacks and data breaches. Authentication and authorization across mobile devices offer convenience, but increase risk by removing a secured enterprise perimeter's constraints. For example, a smartphone's capabilities are enhanced by multi-touch screens, gyroscopes, accelerometers, GPS, microphones, multi-megapixel cameras and ports, allowing the attachment of more devices. These new capabilities change the way users are authenticated and how authorization is provided locally to the device and the applications and services on a network. As a result, the new capabilities are also increasing the number of endpoints that need protection from cyber security threats. Today cybercriminals can hack into cars, security cameras, baby monitors and implanted healthcare devices. And by 2025, there could be more than 75 billion “things” connected to the internet including cameras, thermostats, door locks, smart TVs, health monitors, lighting fixtures and many other devices.

### 2. Current And Emerging Security Threats

New security threats are beginning to emerge as technology continues to develop and grow. The increased use of cloud services in the corporate world will face enormous attacks as per the Security Threat Report 2022 by Sophos. With the emergence of attacks on endpoints, mobile devices will be targeted as corporate businesses are moving to cloud services to provide better service to their customers. It is predicted that the attacking methods will be improvised and adapted to Advance Persistent Threats (APTs). It is also predicted that the attackers will make use of Artificial intelligence (AI) to target the victims with more specialized malwares [1] (Sophos, 2021). While it's certainly critical to establish and enforce an enterprise-wide security policy, a policy alone isn't sufficient to counter the volume and variety of today's mobile threats. In 2019, Verizon conducted a study, with leading mobile security companies, including IBM, Lookout and Wandera, surveying 670 security professionals. The study found that 1 out of 3 of those surveyed reported a compromise involving a mobile device. 47% say remediation was "difficult and expensive," and 64% say they suffered downtime. Companies embracing bring-your-own-device (BYOD) policies also open themselves to higher security risks. They give possibly unsecured devices access to corporate servers and sensitive databases, opening them to attack. Cybercriminals and fraudsters can exploit these vulnerabilities and cause harm or damage to the user and the organization. They seek trade secrets, insider information and unauthorized access to a secure network to find anything that could be profitable


### 3. Cybe

Cybercrime is defined by Dr. Latika Kharb as “a criminal activity committed on the internet and is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money” (Kharb, 2017). Cybercrime can take place against persons, property, and the government. Cybercriminals or hackers commit crimes demanding money from the victims.

#### 3.1 Types of Cyber Crimes

Cybercrimes can be committed through the internet by any medium such as computers or smartphones. There are various kinds of cybercrimes, and the few top crimes include

**Phishing -**

Phishing is a scamming attempt to steal users' credentials or sensitive data, such as credit card numbers. Fraudsters send users emails or short message service (SMS) messages (commonly known as text messages) designed to look as though they're coming from a legitimate source, using fake hyperlinks. [2]

**Malware and Ransomware -**

Mobile malware is undetected software, such as a malicious app or spyware, created to damage, disrupt or gain illegitimate access to a client, computer, server or computer network. Ransomware, a form of malware, threatens to destroy or withhold a victim's data or files unless a ransom is paid to decrypt files and restore

access.

**Cryptojacking -**
Cryptojacking, a form of malware, uses an organization's computing power or individual's computer power without their knowledge to mine crypto currencies such as Bitcoin or Ethereum, decreasing a device's processing abilities and effectiveness

**Cyber stalking -**
Cyber stalking can be defined as a pattern of behavior and acts carried out on the internet or any electronic media to intimidate, alarm, terrify, or harass the victims. [2]

**Email and SMS spoofing -**
The act of creating emails or SMS using a falsified sender address is known as spoofing. In this type of assault, cybercriminals send emails or SMS that have been altered to make them appear to have come from a reliable source (Huseynov, 2021).

**Identity theft -**
Identity theft is taking someone else credentials or personal information and using it to make illicit purchases or conduct financial transactions under a false identity (Nwabineli, Felix, & Aguboshim, 2021).

**Unethical Hacking -**
The process of locating vulnerabilities in the system to gain access to the network to obtain the personal or professional data without authorization. Hacking can be considered unethical when hacking infringes at least one ethical value or moral principle (Chiffelle, 2019).

### 3.2. Mobile Crimes

Mobile crimes are the types of offenses where smartphones or mobile devices are involved in committing crimes against victims. These crimes can be targeted at individuals through phone calls, messages, malware, etc. A few types of Mobile crimes are (Narula, 2019):

**Bluejacking -**
It is the process by which an attacker can send an unwanted or malicious message to any device that is Bluetooth enabled (Techslang, 2022).


**Vishing -**
When an attacker calls a victim and requests information over the phone, this is known as "voice phishing". These assaults can be carried out by leveraging caller ID and social media application data collected from millions of users, together with phone numbers and personal information (S. Jones, E. Armstrong, K. Tornblad, & Namin, 2022).

**Smishing -**
Smishing is a type of phishing in which Attackers send communications via text that looks to be from a reliable source and request that recipients click on a link or share their details via SMS messages instead of sending emails (Njuguna, Kamau, & Kaburu, 2022). [4]



**Mobile Malware -**
Mobile malware is created expressly to target mobile devices like tablets and smartphones to obtain personal data. Mobile user's access unapproved resources to download programs, and the malware present in these sources exposes the user's private data (Aksakalli, 2019).

### 4. Attacks and Threats to Mobile Devices

Security threats [5] are increasing rapidly. Has the security of the technology is increasing, attackers are becoming innovative in breaking these securities. Bring your device (BYOD) is a huge threat to mobile devices. Mobile phishing and ransomware are other major threats faced by the employees of small companies who fail to maintain and follow the policies of such programs. Ransomware distribution using mobile devices running Google's Android OS is on the rise, according to Stu Sjouwerman (NETWORKWORLD, 2022), a cofounder of security training company KnowBe4 LLC. These risks threaten to exploit individuals online or in private and government organizations. These threats can be classified as:

**Application-Based Threats** Applications downloaded from unlicensed content may cause different mobile device cyber threats. Although "malicious apps" are available on the Play Store, they intend to steal the data. These threats include spyware and malware that steal confidential information without people's knowledge.

**Web-Based Threats -** Smartphones enable users to engage in a variety of online activities and are frequently used to access services provided by the Web. Threats based on the web include Phishing, Browser exploit.

**Network-based threats -** Local wireless networks (Wi-Fi, Bluetooth) and cellular networks are both frequently used by mobile devices to connect to the internet. By violating the security on the internet malware could be hosted on the devices. These threats include exploiting the network and WiFi sniffing.

**Unsecured WiFi -** Unsecured WiFi hotspots without a virtual private network (VPN) make mobile devices more vulnerable to cyberattack. Cybercriminals can intercept traffic and steal private information using methods such as man-in-the-middle (MitM) attacks. Cybercriminals can also deceive users into connecting to rogue hotspots, making it easier to extract corporate or personal data.

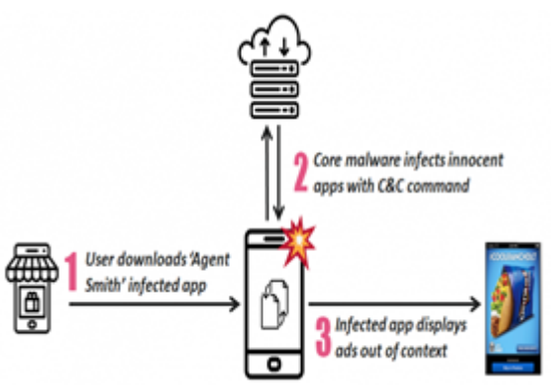
**Outdated Operating Systems -** Older operating systems (OS) usually contain vulnerabilities that have been exploited by cybercriminals, and devices with outdated Oss remain vulnerable to attack. Manufacturer updates often include critical security patches to address vulnerabilities that may be actively exploited. [6]

**Excessive app permissions -** Mobile apps have the power to compromise data privacy through excessive app permissions. App permissions determine an app's functionality and access to a user's device and features, such as its microphone and camera. Some apps are riskier than others. Some can be compromised, and sensitive data can be funneled through to untrustworthy third parties. [7]

5. Case Study - Agent Smith Attack

Agent Smith malware had infected 25 million devices in early 2019, there were around thirty thousand Agent Smith infections in the US and UK. Agent Smith is malware that infected Android devices by replacing the original apps with malicious applications without user knowledge. This malware infected devices around the world including Australia, India, and Pakistan. The malware that spread was a third-party app owned by China. Before April 2019 there was an increase use of the Janus vulnerability to attacks (CVE-2017-13156) (Wu, 2019).

Working of Agent Smith - The victim is lured by the attacker to install the malware-infected app. The app contains encrypted malicious files and is in form of photos, games, or utilities. Once the app is opened, the attacker decrypts and installs the malicious files. The Google Updater was used by malware to disguise its activity (PHILLIPS, 2019). The list of the installed app is created in core malware. In case any app matches the list, it inserts the application with malicious content by updating the app (Rajagopal, 2019).




**Prevention -** Users were advised to uninstall all the infected apps on their mobile phones. The updates and patches were provided by the mobile solutions and monitoring were done from time to time. Users were recommended to use a multilayered mobile security solution to prevent unwanted application downloads and adware on their devices.

**6. How to secure mobile devices**

The core security requirements remain the same for mobile devices as they do for non-mobile computers. In general, the requirements are to maintain and protect confidentiality, integrity, identity and non-repudiation. However, today's mobile security trends create new challenges and opportunities, which require a redefinition of security for personal computing devices. For example, capabilities and expectations vary by device form factor (its shape and size), advances in security technologies, rapidly evolving threat tactics, and device interaction, such as touch, audio and video. IT organizations and Security teams need to reconsider how to achieve security requirements in light of device capabilities, the mobile threat landscape and changing user expectations. In other words, these professionals need to secure multiple vulnerabilities within the dynamic and massively growing mobile device environment. [8-11]

**6.1 Secure Mobile Environment**

A secure mobile environment will offer protection in six primary areas: enterprise mobility management, email security, endpoint protection, VPN, secure gateways and cloud access broker. [12-15]

**Enterprise mobility management** EMM is a collective set of tools and technologies that maintain and manage how mobile and handheld devices are used within an organization for routine business operations.

**Email security -** To protect data from email-based cyber threats such as malware, identity theft and phishing scams, organizations need to monitor email traffic proactively. Adequate email protection includes antivirus, antispam, image control and content control services.

**Endpoint Protection -** With technologies such as mobile, IoT and cloud, organizations connect new and different endpoints to their response environment. Endpoint security includes antivirus protection, data loss prevention, endpoint encryption and endpoint security management.

**VPN -** A virtual private network (VPN) allows a company to securely extend its private intranet over a public network's existing framework, such as the Internet. With a VPN, a company can control network traffic while providing essential security features such as authentication and data privacy.

**Secure Gateways -** A secure gateway is a protected network connection, connecting anything to anything. It enforces consistent internet security and compliance policies for all users regardless of location or device type used, and it keeps unauthorized traffic out of an organization's network

**Cloud Access Broker -** A CASB is a policy enforcement point between users and cloud service providers (CSPs). It monitors cloud-related activity and applies security, compliance and governance rules around cloud-based resources use.

**7. What is an encrypted cell phone?**

Encrypted mobile phones, land line secure phones, encrypted satellite phone, provide a military-grade encryption. These devices are highly reliable and it cannot be cracked or decoded. They are perfect for those who want to protect their own privacy keep data safe and secure. An encrypted cell phone has more features that prevent hackers and spies to access to info on your mobile phone, as the blocking screen does. To better understand how these encrypted devices work, let's consider a blocking screen as a padlock on your house front door. A padlock on your house front door prevents not-invited people to enter the house and stole your personal stuffs; but you have to think to what you would do if someone breaks the padlocks and enters your house. You need several defense levels to really protect your data. Inside the security community, this is called 'defense in depth, and encryption is an important part of it.


**7.1 Types of Encrypted Mobile phones**

There are several types of encrypted mobile phones, each of them has different functionalities coming from highly sophisticated technologies and software that allow users to make phone calls without being listened and then talk securely. Additionally, encrypted smartphones are very requested to manage crypto currencies Bit coin and Altcoin accounts securely; for digital currencies in general. In the range of anti-tapping phones there are two main types of devices: encrypted mobile phones and stealth phones.

**Encrypted mobile phones -** Encrypted mobile phones allows users to make confidential phone calls with military-grade encryption like AES256 or Two Fish 256, only if they are paired with another encrypted mobile phone. It means that these encrypted mobile phones provide the best performance when used paired with another device with the same operating algorithm.

**Stealth Phone -** The Stealth phones instead, works on the mobile phone ID number, known like IMEI (International Mobile Equipment Identity), by changing it any time users decide to. It's a numeric code that identifies the mobile device uniquely, being it a mobile phone or a GSM modem.

**Stealth Phone Plus -** A Stealth phone plus has some additional features as the dual SIM, which are: the protection against active tapping devices, the geolocalization camouflage and an advanced encrypting system of text messages.

**7.2 Advance Encryption Standard**

AES (Advanced Encryption Standard) refers to Military-grade encryption with 256-bit keys. In 2001, AES was announced as the new standard for information security by the National Institute of Standards and Technology (NIST), a unit of the US Commerce Department. Traditionally, military-grade encryption uses a key size equal to or greater than 128 bits. The US government specifies that AES-128 is used for secret (unclassified) information and AES-256 for top secret (classified) information. If an entity handles information on both levels, it usually adopts AES-256 as its standard. The AES-256 block cipher hasn't been cracked yet, but there have been various attempts against AES keys. The first key-recovery attack on full AES was published in 2011 by Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. They used the biclique attack, which is faster than a brute force attack by a factor of about four. However, it was a minor success. The 126-bit key is not widely used, as the lowest key in AES encryption contains 128 bits and it would still take billions of years to brute force the 126-bit key to crack it. That's why this attempt doesn't spell danger for infor-

mation encrypted with the AES. There is no known practical attack that would allow someone to access AES-encrypted data if encryption is implemented correctly.

**How long will the AES last?** According to NIST, no one can be sure how long the AES or any other cryptographic algorithm will remain secure. However, NIST's Data Encryption Standard (known as DES) was a US government standard for approximately 20 years before it became hack able. The AES supports significantly larger key sizes than what DES supports. Barring any attacks against AES that are faster than key exhaustion, and even with future advances in technology, AES has the potential to remain secure well beyond 20 years.

**7.3 Do you need military-grade security?**
Many skeptics would say that you don't need it as other encryption algorithms would do a good job too. However, no industry or service is immune to attacks and services that store sensitive information, such as passwords or financial data, should not apply anything less than the recommended standard. Back when the NIST presented this standard to the public in 2001, they already expected that the private sector would widely adopt it. They saw and still see it as a benefit to millions of consumers and businesses for protecting their sensitive information. So yes, if you want to show that you care about your users and their personal data, you must use the best encryption available.

**8. User Requirement or Policy Constraints**
Seven governments from across the world have started a new campaign to try and persuade big tech companies to reduce the level of security they offer to customers using their services. The seven -- US, UK, Canada, Australia , New Zealand, India and Japan -- are worried that the use of end-to-end encryption makes it impossible for tech companies to identify dangerous content like terrorist propaganda and attack planning, and makes it harder for police to investigate serious crimes and protect national security.

Their statement starts boldly: "We, the undersigned, support strong encryption", saying that it plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security, and in repressive states protects journalists, human rights defenders and other vulnerable people. Then, of course, comes the big caveat: "We urge industry to address our serious concerns where encryption is applied in a way that wholly precludes any legal access to content." The sort of end-to-end encryption that means messages can't be intercepted, or that a hard drive can never be read without the key, "pose significant challenges to public safety", the seven governments warn. This of course is where things get trickier. These governments want tech companies to make it possible to act against illegal content and activity, but with no reduction to safety -- something that tech companies insist is impossible. "We challenge the assertion that public safety cannot be protected without compromising privacy or cyber security. We strongly believe that approaches protecting each of these important values are possible and strive to work with industry to collaborate on mutually agreeable solutions," the statement concludes. Tech companies argue that end-to-end encryption protects users' privacy rights, and it to weaken it -- by creating a so-called 'backdoor' that would allow the authorities to look at messages -- would put all sorts of private communications at risk from hackers and force them to decide whether to hand over messages to oppressive regimes. End-to-end encryption makes the tech companies' lives easier, and also allows them to claim the moral high-ground when it comes to privacy. So is there anything new in this? Governments have been half-heartedly trying to refight the crypto wars for years now, with little success -- largely because they know that coming up with a fix for this is hard. They know it's all but impossible to ban the use of end-to-end encryption. Sure, you could pass laws to ban it, and maybe block encrypted apps from local app stores if they used it, or make it illegal to possess them. But that's insanely hard to justify and even harder to enforce -- even for states like Russia, which have tried to ban encrypted services. And even if you did go for a ban, organized crime would simply get hold of encryption on the black market or from abroad, and would be just as well-protected as ever. But the average person on the street would be unable to access strong encryption, and would be more at risk of hacking as a result. A policy that makes the average person less secure, while doing little to tackle the real problem, seems unlikely to gain much support. Imagine being the politician who has to explain to the country that their data has just been scooped up by a foreign power as a result. The UK's GCHQ has come up with an idea called **'ghost protocol'**, which would add the government as a secret eavesdropper into every call. But although GCHQ's scheme has technical merit, if tech companies said 'yes' to one agency they would struggle to exclude others. That's because governments will inevitably over-reach and use such powers to increase their general surveillance. It's worth remembering that many of these tech companies introduced end-to-end encryption precisely because governments were cheerfully snooping on everyone's conversations in the first place. Many would say it's brazen of governments to now ask us to trust them again.

**9. Conclusion**
Security threats related to mobile devices are the most critical. There are many different kinds of software security hazards, as well as several risks connected to mobile devices with ways to reduce these risks. Security specialists face challenges in defending against mobile threats due to the tremendous growth of mobile threats. Social engineering attacks are one of the biggest security risks that an organization faces. Corporate companies are more prone to insider threats but they deny mentioning or discussing these threats fearing the loss of business. In addition and on a serious note End-to-end encryption creates real and tragic problems for police and the victims of crime, yet governments have not made a decent case for making us all less secure in response to those problems. Still, governments are increasingly conscious of the impact of big tech companies, and are increasingly willing to take them on. It may only take a few high-profile situations where strong encryption prevents a terrible crime from being stopped or investigated, for governments to think that public opinion can be shifted in their direction. This paper reviewed the kinds of threats in detail, discussed the countermeasures and some policy constraints in implementation of end to end encryption owing to various governments stand of posing significant challenges to public safety.

**REFERENCES**

1. Sophos. (2021). Sophos 2022 Threat Report..
2. Abdul Quadir Md, Dibyanshu Jaiswal, Jay Daftari, Sabireen Haneef, Celestine Iwendi, & Sanjiv Kumar Jain. (2022). Efficient Dynamic Phishing Safeguard System Using Neural Boost Phishing Protection. (A. Gangopadhyay, Ed.) MDPI, 1-17.
3. Nwabineli, T. C., Felix, C., & Aguboshim, F. (2021). Strategies for Identity Theft Prevention and Countermeasures in Nigeria:A Narrative Study. International Journal of Advances in Engineering and Management (IJAEM), 3(1), 826-832.
4. Njuguna, D., Kamau, J., & Kaburu, D. (2022). A Review of Smishing Attaks Mitigation Strategies. International Journal of Computer and Information Technology (, 11(1), 9-13.
5. Gilibrays, G., Matovu, D., Egwar, A. A., & Bongomin, O. (2022). An application-based framework for curbing mobile phone-related crimes: Results of a preliminary study in Eastern Uganda. 1-15.
6. R. Mistry, N., Dahiya, M., & P. Sanghvi, H. (2013). Preventive Actions to Emerging Threats in Smart Devices Security. The International Journal of FORENSIC COMPUTER SCIENCE, 20-26.
7. Lemos, R. (2022). DarkReading. Retrieved from https://www.darkreading.com/endpoint/mobile-threats skyrocket
8. Vashisht, S., Gupta, S., Singh, D., & Mudgal, A. (2016). EMERGING THREATS IN MOBILE COMMUNICATION SYSTEM. International Conference on Innovation and Challenges in Cyber Security (pp. 41-44). IEEE.
9. Omer Faruqe Jubaer, M. S., Rumon, A. A., Khan, F. R., Suma, T. A., Dhar, P., & Badhan, P. D. (n.d.). Cyber Stalking is a Cybercrime or not: Hosting a new cybercrime. online Bibliophiles
10. Kharb, L. (2017). Cyber Crimes Becoming Threat to Cyber Security. International Journal of Engineering and Management Research, 7(2), 48-51.
11. Hakhroo, B. (2020). A STUDY ON TYPES OF CYBER CRIMES AND CYBER ATTACKS IN INDIA. International Journal of Creative Research Thoughts (IJCRT), 8(11), 1257-1260.
12. Narula, K. (2019). Retrieved Nov 18, 2022, from legitly.in: https://legitly.in/2019/08/mobile-phone crimes/
13. Aksakalli, I. K. (2019). Using convolutional neural network for Android malware detection. information and computer technologies, 29-35.
14. S. Jones, K., E. Armstrong, M., K. Tornblad, M., & Namin, A. S. (2022). How Social Engineers User Persuasion Principles During Vishing Attacks. Information and Computer Security.
15. Wu, L. (2019). Trendmicro. Retrieved Nov 20, 2022, from https://www.trendmicro.com/vinfo/us/security/news/cy bercrime-and-digital- threats